



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,823	04/14/2004	Keisuke Takemori	61230 (47762)	6683

7590 09/03/2008  
Edwards & Angell, LLP  
Intellectual Property Practice Group  
P.O. Box 55874  
Boston, MA 02205

EXAMINER
----------

OKORONKWO, CHINWENDU C

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

09/03/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<p align="center"><b>Advisory Action</b> <b>Before the Filing of an Appeal Brief</b></p>	<b>Application No.</b> 10/824,823	<b>Applicant(s)</b> TAKEMORI ET AL.	
	<b>Examiner</b> CHINWENDU C. OKORONKWO	<b>Art Unit</b> 2136	

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 01 August 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires \_\_\_\_\_ months from the mailing date of the final rejection.  
 b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

#### AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
 (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);  
 (b) ☐ They raise the issue of new matter (see NOTE below);  
 (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
 (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: \_\_\_\_\_. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).  
 5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.  
 6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).  
 7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.  
 The status of the claim(s) is (or will be) as follows:  
 Claim(s) allowed: \_\_\_\_\_.  
 Claim(s) objected to: \_\_\_\_\_.  
 Claim(s) rejected: \_\_\_\_\_.  
 Claim(s) withdrawn from consideration: \_\_\_\_\_.

#### AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).  
 9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).  
 10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

#### REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet.  
 12. ☒ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). 20080807  
 13. ☐ Other: \_\_\_\_\_.

/Nasser G Moazzami/  
 Supervisory Patent Examiner, Art Unit 2136

Continuation of 11. does NOT place the application in condition for allowance because: In response to Applicant argument that the Douglas in view of Maier references do not teach or suggest support apparatus arranged separately from the intrusion detection system, the Examiner respectfully disagrees citing column 4 lines 1-11 of Douglas, which recites, "the present invention 20 is a modular system for detecting, filtering and providing notice about attack events associated with network security. The present invention 20 is a host-based IDS (HIDS) sensor that is capable of monitoring resources on the deployed host and activity forwarded to the host via SNMP or SYSLOG. The present invention 20 can be run stand-alone or fully integrated into an IDS. Events can either be stored locally on the HIDS sensor 20 or forwarded to EFPs 18 and analyzed with the IDS reporting tools." Thus Douglas does indeed suggest an apparatus and method arranged separately from the intrusion detection system in "stand-alone" mode, the apparatus being the system as a whole including the computer (server) upon which the modules execute and operate.

In response to Applicant argument that the Maier does not teach or suggest a database that "stores and manages logs collected by the log collection section," the Examiner respectfully disagrees citing column 2 lines 23-32, which recites "a database computer system having memory, residing in a plurality of interconnected computer nodes, for storing database tables." Further the Douglas reference discloses in column 6 lines 1-6 an "[event alerting engine] EAE 26 receives all HIDS sensor 20 events generated by each of the EDE 24 modules after any filtration by EFE 24 modules is finished ... EAE 26 modules provided by Enterasys include ring buffer alerting module 26A, replication agent alerting modules 26B, Dragon database (DB) alerting module 26C, export log alerting module 26D, SNMP trap alerting module 26E, and hexadecimal dump alerting module 26F. A customer can develop an EAE 26 module to record events directly to an in-house database, perform event correlation, or feed events to a locally-installed windows application."

The Applicant arguments have not overcome the references of record.